DKIM Sender Signing ~~Policy~~

Practices

Jim Fenton <fenton@cisco.com>

12 July 2006

SSP: The Problem

- **“I got a message that is unsigned. How do I know if it is legitimate?”**

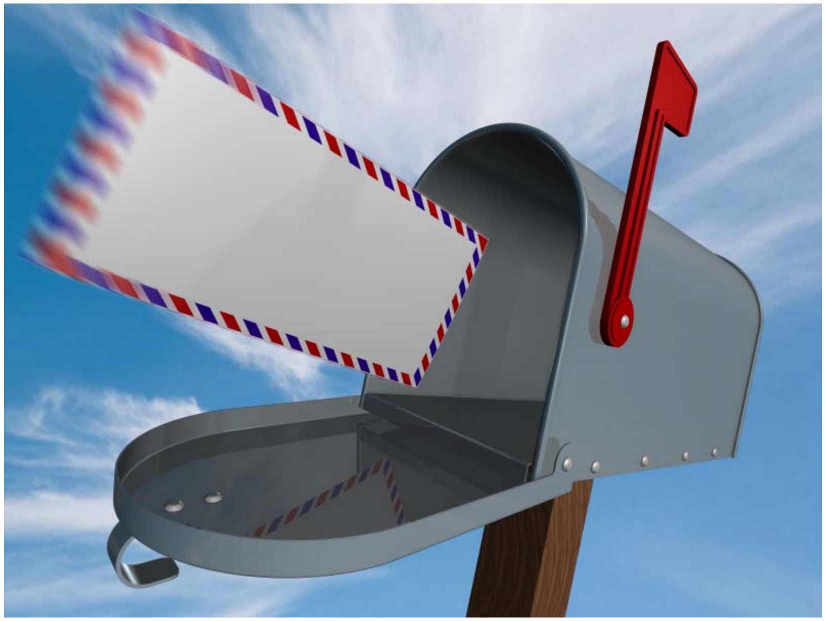
What About Unsigned Messages?

- **Does the author’s domain:**

  Send mail?

  Sign all their mail?

- **If these practices are inconsistent with the received message, it’s “suspicious”**



Suspicious

- Messages that aren’t consistent with author’s practices
- Intentionally vague – doesn’t say anything about what to do

Third Parties

- Messages can be signed by other than the author’s domain
  - Mailing lists that modify messages
  - “Mail this article to a friend” applications
- Author [domain] may avoid such agents
- “No third-party” practice reflects this
  - Usable by only a few high-value domains
  - Example: mail from banks to customers

Caveats

- Some legitimate messages will likely be suspicious

  Messages through lists that munge messages and don’t re-sign them

- It’s probably not good to over-react to suspicious messages

  Deleting them outright

Finding the SSP

- SSP is found using the From address in the message
- example.com SSP is located at _policy._domainkey.example.com
- SSP lookup is not needed if a valid origination address signature is found

  SSP only offers information that is relevant in its absence

Defined Practices*

Symbol	Proposed Name	Meaning
~	NEUTRAL	Signs some mail
-	STRONG	Signs all mail
!	EXCLUSIVE	Signs all mail; third-party signatures should not be considered valid
.	NEVER	Entity never sends mail
^	USER	Repeat query at user level

* As of draft-allman-dkim-ssp-01

Open questions

- How DKIM-specific should SSP be?

  Mailing practices? Broader messaging practices?

- Location and form of SSP

  Prefixed DNS TXT record [current draft]   Syntax?

  New DNS resource record, probably without prefix

- Other policies?

  Name other domains that send mail on author’s behalf

  “I don’t sign anything”

  “I don’t sign everything, but don’t accept third-party sigs”

More open questions

- **User-level practices**

  Useful?

  Out-of-scope and costly?

- **Reporting address**

  Local-part only to avoid abuse?

  Inappropriate and likely to be abused?